

IN THE CLAIMS:

1 1. (PREVIOUSLY PRESENTED) A method for implementing port-based network ac-
2 cess control at a shared media port in an intermediate node, the shared media port being a
3 physical interface coupled to a plurality of client nodes, the method comprising:

4 partitioning the shared media port into a plurality of logical subinterfaces, wherein
5 a logical subinterface is a logical division of a physical interface, each logical subinter-
6 face dedicated to providing access to a different network or subnetwork accessible
7 through the intermediate node;

8 receiving a data packet at the shared media port from a first client node;

9 associating the received data packet with a first logical subinterface in the plural-
10 ity of logical subinterfaces;

11 determining whether the first client node is authenticated to communicate over the
12 first logical subinterface's dedicated network or subnetwork;

13 if the first client node is determined to be authenticated to communicate over the
14 first logical subinterface's dedicated network or subnetwork, forwarding the received
15 data packet over the first logical subinterface's dedicated network or subnetwork;

16 receiving a second data packet at the shared media port from a second client node;

17 associating the second received data packet with the first logical subinterface;

18 determining whether the second client node is authenticated to communicate over
19 the first logical subinterface's dedicated network or subnetwork; and

20 if the second client node is determined to not be authenticated to communicate
21 over the first logical subinterface's dedicated network or subnetwork, preventing the sec-
22 ond received data packet from being forwarded over the first logical subinterface's dedi-
23 cated network or subnetwork, while still allowing data packets from the first client node
24 to be forwarded if the first client node is determined to be authenticated.

1 2. (ORIGINAL) The method according to claim 1, further comprising:

2 performing at least one of dropping the received data packet or reclassifying the
3 received data packet to a different logical subinterface, if the first client node is deter-
4 mined not to be authenticated to communicate over the first logical subinterface's dedi-
5 cated network or subnetwork.

1 3. (ORIGINAL) The method according to claim 1, wherein the first logical subinterface's
2 dedicated network or subnetwork is a virtual private network (VPN).

1 4. (ORIGINAL) The method according to claim 1, wherein a logical subinterface in the
2 plurality of logical subinterfaces is dedicated to providing access to the Internet.

1 5. (ORIGINAL) The method according to claim 1, wherein the step of determining
2 whether the first client node is authenticated to communicate over the first logical subin-
3 terface's dedicated network or subnetwork further comprises:

4 parsing a source media access control (MAC) address from the received data
5 packet;

6 indexing an entry in a MAC filter associated with the shared media port based on
7 the value of the parsed source MAC address;

8 identifying an authentication state stored in the indexed MAC-filter entry; and

9 determining whether the first client node is authenticated to communicate over the
10 first logical subinterface's dedicated network or subnetwork based on the authentication
11 state stored in the indexed MAC-filter entry.

1 6. (ORIGINAL) The method according to claim 5, wherein the MAC filter is organized
2 as a hash table.

1 7. (ORIGINAL) The method according to claim 1, further comprising:

2 parsing a destination Internet Protocol (IP) address from the received data packet;

3 comparing the parsed destination IP address to one or more IP addresses stored in
4 an IP filter associated with the shared media port; and

5 if the parsed destination IP address matches an IP address stored in the IP filter,
6 forwarding the received data packet over the first logical subinterface's dedicated net-
7 work or subnetwork, even if the first client node is determined not to be authenticated to
8 communicate over that network or subnetwork.

1 8. (ORIGINAL) The method according to claim 1, wherein the step of associating the
2 received data packet with the first logical subinterface, further comprises:

3 locating an entry in a routing table configured to store routing information associ-
4 ated with the received data packet; and

5 associating the received data packet with the first logical subinterface based on
6 the contents of the routing-table entry.

1 9. (ORIGINAL) The method according to claim 1, further comprising:

2 receiving an authentication request from the first client node at the shared media
3 port;

4 in response to receiving the authentication request, creating a MAC filter associ-
5 ated with the shared media port if the MAC filter has not already been created;

6 copying a source MAC address stored in the received authentication request into
7 an appropriate entry in the MAC filter;

8 forwarding the received authentication request to an authentication service;

9 receiving a response from the authentication service, the response identifying an
10 authentication state associated with the first client node; and

11 storing the authentication state into the same MAC-filter entry into which the
12 source MAC address was copied.

1 10. (ORIGINAL) The method according to claim 9, wherein the step of copying the
2 source MAC address into an appropriate MAC-filter entry further comprises:

indexing an entry in the MAC filter based on the result of applying a hash function to the source MAC address; and
storing the source MAC address at the indexed MAC-filter entry.

11. (ORIGINAL) The method according to claim 9, wherein the received authentication request is an 802.1X authentication request.

12. (ORIGINAL) The method according to claim 9, further comprising:
sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node fails to authenticate at the shared media port a predetermined number of times.

13. (ORIGINAL) The method according to claim 9, further comprising:
sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node's authentication state changes from an authenticated state to an unauthenticated or unknown state.

14. (PREVIOUSLY PRESENTED) An intermediate node for implementing port-based network access control in a network containing a plurality of client nodes, the intermediate node comprising:
a processor;
a shared media port that is a physical interface for receiving a data packet from a first client node, and a second data packet from a second client node, in the plurality of client nodes; and
a memory adapted to store instructions for execution by the processor, at least a portion of the instructions defining a network operating system configured to perform the steps of:
partitioning the shared media port into a plurality of logical subinterfaces, wherein a logical subinterface is a logical division of a physical interface, each

13 logical subinterface dedicated to providing access to a different network or sub-
14 network accessible through the intermediate node;

15 associating the data packet received from the first client node with a first
16 logical subinterface in the plurality of logical subinterfaces;

17 determining whether the first client node is authenticated to communicate
18 over the network or subnetwork to which the first logical subinterface provides
19 dedicated access;

20 forwarding the received data packet over the first logical subinterface's
21 dedicated network or subnetwork only if the first client node is determined to be
22 authenticated to communicate over that network or subnetwork

23 associating the second received data packet with the first logical subinter-
24 face;

25 determining whether the second client node is authenticated to communi-
26 cate over the first logical subinterface; and

27 preventing the second received data packet from being forwarded over the
28 first logical subinterface's dedicated network or subnetwork if the second client
29 node is determined to not be authenticated to communicate over that network or
30 subnetwork, while still allowing data packets from the first client node to be for-
31 forwarded over that network or subnetwork if the first client node is determined to be
32 authenticated.

1 15. (ORIGINAL) The intermediate node according to claim 14, wherein:

2 the memory is further adapted to store a MAC filter containing one or more en-
3 tries configured to store at least a MAC address and an authentication state, and

4 the network operating system is further configured to perform the steps:

5 receiving an authentication request from the first client node at the
6 shared media port;

7 copying a source MAC address stored in the received authentica-
8 tion request into an appropriate entry in the MAC filter;

9 forwarding the received authentication request to an authentication
10 service;
11 receiving a response from the authentication service, the response
12 identifying an authentication state associated with the first client node; and
13 storing the authentication state into the same MAC-filter entry into
14 which the source MAC address was copied.

1 16. (ORIGINAL) The intermediate node according to claim 14, wherein:
2 the memory is further adapted to store an IP filter containing a list of IP addresses,
3 and
4 the network operating system is further configured to perform the steps:
5 parsing a destination IP address from the received data packet;
6 comparing the parsed destination IP address to one or more IP ad-
7 dresses stored in an IP filter associated with the shared media port; and
8 if the parsed destination IP address matches an IP address stored in
9 the IP filter, forwarding the received data packet over the first logical sub-
10 interface's dedicated network or subnetwork, even if the first client node is
11 determined not to be authenticated to communicate over that network or
12 subnetwork.

1 17. (ORIGINAL) The intermediate node according to claim 14, wherein:
2 the memory is further adapted to store a MAC filter containing one or more en-
3 tries configured to store at least a MAC address and an authentication state, and
4 the network operating system is further configured to perform the steps:
5 parsing a source MAC address from the received data packet;
6 indexing an entry in a MAC filter associated with the shared media
7 port based on the value of the parsed source MAC address;
8 identifying an authentication state stored in the indexed MAC-filter
9 entry; and

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork based on the authentication state stored in the indexed MAC-filter entry.

18. (PREVIOUSLY PRESENTED) An apparatus that implements port-based network access control at a shared media port, the shared media port being a physical interface coupled to a plurality of client nodes, the apparatus comprising:

means for partitioning the shared media port into a plurality of logical subinterfaces, wherein a logical subinterface is a logical division of a physical interface, each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node;

means for receiving a data packet at the shared media port from a first client node;

means for associating the received data packet with a first logical subinterface in the plurality of logical subinterfaces;

means for determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork;

means for forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork;

means for receiving a second data packet at the shared media port from a second client node;

means for associating the second received data packet with the first logical subinterface;

means for determining whether the second client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork; and

means for preventing the second received data packet from being forwarded over the first logical subinterface's dedicated network or subnetwork, while still allowing data packets from the first client node to be forwarded.

1 19. (ORIGINAL) The apparatus according to claim 18, wherein the means for determin-
2 ing whether the first client node is authenticated to communicate over the first logical
3 subinterface's dedicated network or subnetwork further comprises:

4 means for parsing a source MAC address from the received data packet;

5 means for indexing an entry in a MAC filter associated with the shared media port
6 based on the value of the parsed source MAC address;

7 means for identifying an authentication state stored in the indexed MAC-filter en-
8 try; and

9 means for determining whether the first client node is authenticated to communi-
10 cate over the first logical subinterface's dedicated network or subnetwork based on the
11 authentication state stored in the indexed MAC-filter entry.

1 20. (ORIGINAL) The apparatus according to claim 18, further comprising:

2 means for parsing a destination IP address from the received data packet;

3 means for comparing the parsed destination IP address to one or more IP ad-
4 dresses stored in an IP filter associated with the shared media port; and

5 means for forwarding the received data packet over the first logical subinterface's
6 dedicated network or subnetwork, even if the first client node is determined not to be au-
7 thenticated to communicate over that network or subnetwork.

1 21. (ORIGINAL) The apparatus according to claim 18, wherein the means for associating
2 the received data packet with the first logical subinterface, further comprises:

3 means for locating an entry in a routing table configured to store routing informa-
4 tion associated with the received data packet; and

5 means for associating the received data packet with the first logical subinterface
6 based on the contents of the routing-table entry.

1 22. (ORIGINAL) The apparatus according to claim 18, further comprising:

2 means for receiving an authentication request from the first client node at the
3 shared media port;

4 means for creating a MAC filter associated with the shared media port if the MAC
5 filter has not already been created;

6 means for copying a source MAC address stored in the received authentication
7 request into an appropriate entry in the MAC filter;

8 means for forwarding the received authentication request to an authentication ser-
9 vice;

10 means for receiving a response from the authentication service, the response iden-
11 tifying an authentication state associated with the first client node; and

12 means for storing the authentication state into the same MAC-filter entry into
13 which the source MAC address was copied.

1 23. (ORIGINAL) The apparatus according to claim 22, wherein the received authentica-
2 tion request is an 802.1X authentication request.

1 24. (PREVIOUSLY PRESENTED) A computer-readable media including instructions
2 for execution by a processor, the instructions for a method of implementing port-based
3 network access control at a shared media port in an intermediate node, the shared media
4 port being a physical interface coupled to a plurality of client nodes, the method compris-
5 ing the steps:

6 partitioning the shared media port into a plurality of logical subinterfaces, wherein
7 a logical subinterface is a logical division of a physical interface, each logical subinter-
8 face dedicated to providing access to a different network or subnetwork accessible
9 through the intermediate node;

10 receiving a data packet at the shared media port from a first client node;

11 associating the received data packet with a first logical subinterface in the plural-
12 ity of logical subinterfaces;

13 determining whether the first client node is authenticated to communicate over the
14 first logical subinterface's dedicated network or subnetwork;

15 if the first client node is determined to be authenticated to communicate over the
16 first logical subinterface's dedicated network or subnetwork, forwarding the received
17 data packet over the first logical subinterface's dedicated network or subnetwork;

18 receiving a second data packet at the shared media port from a second client node;
19 associating the second received data packet with the first logical subinterface;

20 determining whether the second client node is authenticated to communicate over
21 the first logical subinterface's dedicated network or subnetwork; and if the second
22 client node is determined to not be authenticated to communicate over the first logical
23 subinterface's dedicated network or subnetwork, preventing the second received data
24 packet from being forwarded over the first logical subinterface's dedicated network or
25 subnetwork, while still allowing data packets from the first client node to be forwarded if
26 the first client node is determined to be authenticated.

1 25. (PREVIOUSLY PRESENTED) An apparatus comprising:

2 a shared media port that is a physical interface and has a trusted subinterface con-
3 figured to provide access to a trusted network or subnetwork and an untrusted subinter-
4 face configured to provide access to an untrusted network or subnetwork, wherein a sub-
5 interface is a logical division of a physical interface;

6 an authenticator configured to receive authentication requests from a plurality of
7 client nodes and in response the authentication requests to independently assign to each
8 of the plurality of client nodes an authentication state; and

9 a media access control (MAC) filter configured to maintain an entry for each cli-
10 ent node indicating the authentication state of the client node and a MAC address of the
11 client node, and in response to receipt of a data packet from a particular client node di-
12 rected to the trusted subinterface, to index to an entry in the MAC filter based on a source
13 MAC address of the data packet, to identify the authentication state of the particular cli-

14 ent node stored in the indexed MAC-filter entry, and to determine whether the particular
15 client node is authenticated to communicate over the trusted subinterface, and, if so, to
16 permit the particular client node to access the trusted subinterface,
17 wherein the media access control (MAC) filter grants client nodes access on a cli-
18 ent-by-client basis.

1 26. (PREVIOUSLY PRESENTED) The apparatus of claim 25, wherein the media ac-
2 cess control (MAC) filter is further configured to redirect the data packet from the par-
3 ticular client node directed to the trusted subinterface to the untrusted subinterface if the
4 particular client node is not authenticated to communicate over the trusted subinterface.

1 27. (PREVIOUSLY PRESENTED) The apparatus according to claim 25, wherein the
2 trusted network or subnetwork is a virtual private network (VPN).

1 28. (PREVIOUSLY PRESENTED) The apparatus according to claim 25, wherein the
2 untrusted network or subnetwork is the Internet.

1 29. (PREVIOUSLY PRESENTED) A method for implementing port-based network ac-
2 cess control at a shared media port in an intermediate node, the shared media port being a
3 physical interface coupled to a plurality of client nodes, the method comprising:

4 partitioning the shared media port into a plurality of logical subinterfaces by logi-
5 cally dividing the shared media port into subinterfaces, each logical subinterface dedi-
6 cated to providing access to a different network or subnetwork accessible through the in-
7 termediate node;

8 receiving a data packet at the shared media port from a first client node;

9 associating the received data packet with a first logical subinterface in the plural-
10 ity of logical subinterfaces;

11 determining whether the first client node is authenticated to communicate over the
12 first logical subinterface's dedicated network or subnetwork; and

13 if the first client node is determined to be authenticated to communicate over the
14 first logical subinterface's dedicated network or subnetwork, forwarding the received
15 data packet over the first logical subinterface's dedicated network or subnetwork.

1 30. (PREVIOUSLY PRESENTED) The method according to claim 29, further compris-
2 ing:

3 performing at least one of dropping the received data packet or reclassifying the
4 received data packet to a different logical subinterface, if the first client node is deter-
5 mined not to be authenticated to communicate over the first logical subinterface's dedi-
6 cated network or subnetwork.

1 31. (PREVIOUSLY PRESENTED) The method according to claim 29, wherein the first
2 logical subinterface's dedicated network or subnetwork is a virtual private network
3 (VPN).

1 32. (PREVIOUSLY PRESENTED) The method according to claim 29, wherein a logical
2 subinterface in the plurality of logical subinterfaces is dedicated to providing access to
3 the Internet.